



Office of Thrift Supervision

Department of the Treasury

1700 G Street, N.W., Washington, DC 20552 • (202) 906-6000

PRIVACY PREPAREDNESS CHECK-UP

The Gramm-Leach-Bliley Act of 1999, also known as the Financial Services Modernization Act, instituted significant changes to the laws governing financial institutions. Title V of the Act set forth provisions addressing the rights of a consumer with respect to privacy of non-public financial information. The implementing regulation, 12 CFR Part 573, describes the obligation of the financial institution to inform the consumer of its information-sharing practices with both affiliated and non-affiliated third parties; the rights of the consumer, subject to certain exceptions, to opt-out of such sharing; and the security provided for consumer information by the institution.

As part of the rule-making process, the OTS and its fellow federal agencies solicited public comment. Many industry members commented that the rule's provisions would require extensive and costly adaptation measures. The agencies sought to balance the rule's important privacy objectives with the prospective burden on the industry and determined that some accommodations were necessary. Consequently, despite the rule's effective date of November 13, 2000, full compliance is not mandatory until July 1, 2001. However, during the interim period, financial institutions are **"expected to begin compliance efforts promptly, to use the period prior to June 30, 2001 to implement and test their systems, and to be in full compliance by July 1, 2001."** 65 Federal Register 35162, 35185 (June 1, 2000).

The purpose of this Privacy Preparedness Check-up is to provide you, the examiner, with a number of questions to assist you in determining the efforts of institutional management to achieve compliance with the privacy rule. After discussing these questions with management and considering any other related information offered by management, you should be able to determine the "preparedness" of the institution and to provide management with an assessment. Management should be mindful that many of the rule's provisions, such as the dissemination of an initial privacy notice and, an opt-out notice and the expiration of a reasonable opt-out time period, must have been accomplished **prior to** July 1, 2001. Although the extent of compliance efforts will vary among entities depending on their information-sharing practices, affiliate relationships and organizational size, **all** institutions should currently be working toward the mandatory compliance date. No institution is excepted from the Act's requirements. Even if the thrift has no expectation of sharing consumer information, it is required to have and disclose its privacy policy.

The well prepared institution will develop and execute an approach or plan to take it from understanding its obligations under the privacy rule to implementing the policies, practices, controls and systems that will assure timely compliance. The Privacy Preparedness Check-up is

intended to be a general guide, with a broad scope capturing the principal components of a sound plan of action. However, the guide is not a requirement for rigid formality. Rather it serves as a benchmark for institutions and examiners to apply to a wide range of operations in evaluating whether thrifts are making considered progress toward effective compliance management policies and systems.

The Check-up is not a set of examination procedures. The FFIEC agencies are preparing a consensus set of examination procedures that will be issued later this year. Those procedures will be employed when the compliance deadline of July 1, 2001 has been reached. Of course, once published, the procedures can be a valuable resource to aid institution efforts to evaluate the sufficiency of the policies they create in the development stage of their preparedness plan. In the interim, institutions and all examiners should become familiar with the privacy regulation. OTS compliance examiners are undergoing training as part of their regional conferences and Washington will support their continued education.

The Check-up will be performed on-site during compliance examinations scheduled in the remainder of the current year. In the first third of 2001, OTS will make on-site or off-site contact with all other institutions to complete its survey of thrift industry preparedness. The goal of the program is to encourage sound compliance planning--not to enforce a uniform approach. In fact, an important key to understanding the new privacy rule is to recognize the flexibility it provides for tailoring each institution's substantive privacy policies. Accordingly, the Preparedness Check-up should be applied in a way that accommodates that flexibility.

Examiner and industry feedback is welcome, as is community input. The public may address questions or comments about this Check-up to privacy.checkup@ots.treas.gov. We will incorporate improvements to the Check-up in a revised version for use during the review conducted in 2001.

Everyone should recognize that implementing the new privacy rule is going to be a learning experience for all concerned. It is likely that situations will come to our attention that will require staff interpretation and interagency coordination. We will endeavor to make the process as responsive as our resources allow. Please watch for bulletins and other types of guidance to be issued as our experience grows over the coming months.

PLAN to meet the deadline

Every institution should know how it is going to go about the process of achieving timely compliance and be able to articulate its approach to reaching that goal.

Plan Structure: Has the institution articulated an approach to preparing for privacy rule compliance?

- Has the institution's approach been presented to and endorsed by senior management and the Board?

- Has the institution's approach to preparedness been communicated to management and appropriate staff?

An Institution should approach compliance by following a sensible sequence of steps that enable it to make successive judgments from an informed perspective.

Plan Components: Does the plan cover the following steps?

- Taking an inventory of existing information collection standards, uses of customer information, policies and practices for sharing information and controls for monitoring compliance.
- A process for evaluating gaps or deficiencies between existing practices and requirements for future compliance.
- Developing new policies, practices and controls to assure future compliance.
- A schedule for testing, implementing and monitoring new policies, practices, systems and controls.

Institutions should have someone in charge of their privacy preparedness plan who is held accountable for meeting the deadline.

Responsibility and Accountability: How is responsibility for accomplishing the plan organized?

- Are particular officers assigned responsibility for preparing for compliance?
- Are institutional units involved in the preparedness efforts aware of their respective roles and responsibilities, and subject to effective management coordination?
- If outside contractors or advisors are relied on for assuring the institution's compliance, are their responsibilities coordinated and monitored by institution management?
- What role does the Board of Directors play in ensuring the institution accomplishes its plans to meet the compliance deadline?

Institutions need to measure progress toward the compliance deadline.

Timetable and Milestones: Has the institution established a timeline or schedule for fulfilling the steps in its plan?

- Does the timeline afford customers a reasonable time to exercise, before July 1, 2001, whatever opt-out rights may be offered?
- Are intermediate milestones used to create an orderly sequence for achieving compliance?
- At this time, how well are milestones being met and how are shortfalls addressed?

INVENTORY current practices

Institutions need to know their current uses of consumer information in order to understand the impact of the new privacy rule on their operations. Therefore, as part of the plan does the institution

- Identify the types of information it collects from consumers and the uses made of such information?
- Identify its current consumer privacy policies and what has been disclosed to existing consumers about such policies?
- Determine how it handles consumer information differently when dealing with affiliate and non-affiliates?
- Take stock of existing agreements with third parties about the use and reuse of consumer information?
- Identify the various data systems that store or access consumer information and ascertain practices of service providers where they are relied on?
- Identify the level of staff knowledge and training about the institution's information sharing practices?
- Determine the level of security and confidentiality that applies to various forms of consumer information?

EVALUATE current practices/policies

As part of its plan the institution should evaluate its current practices against the requirements of the new privacy rule. Therefore, as part of the plan does management

- Become fully versed in the requirements of the new privacy rule to conduct an evaluation of its obligations going forward?
- Categorize consumer information in accordance with regulatory definitions giving due regard to the need to have a reasonable basis to believe certain information is publicly available?
- Determine how current information-sharing practices will be impacted by the new privacy obligations? Is due consideration given to the differences in types of information shared, the purposes for sharing and parties with whom information is shared?
- Review existing policies or procedures for compliance with the provisions of the rule?
- Identify any deficiencies between current information sharing practices and policies and the requirements of the new rule?
- Consider alternative means of achieving compliance and evaluate their costs?
- Recognize the flexibility available in establishing the institution's privacy policies, including giving due consideration to:
 - Whether to share, to begin to share or to discontinue sharing information with nonaffiliated third parties or with affiliates?

- The reactions and receptivity of its customers to different policies for information sharing?
- The prospective information sharing practices of its competitors?
- Review the contractual agreements currently in effect with nonaffiliated third parties? Will legal counsel and/or the regulatory compliance department be involved in the review process? Will the impact of the grand-fathering provisions of the rule be taken into account with respect to third party contracts?

As part of the plan's evaluation of information systems does management

- Identify the information systems resource needs required for complying with the privacy rule?
- Determine the readiness of service providers to support the institution's privacy policies?
- Evaluate how much and what kind of training will be required to acquaint responsible staff with new compliance requirements?
- Measure existing information security against new interagency guidance?

DEVELOP privacy policies, practices and expertise

The plan should take the process of preparedness from evaluation to developing the necessary policies and systems that fulfill the compliance obligations of the institution. Therefore, does the plan assure that

- The development stage is built around the articulation of a comprehensive consumer information privacy policy that contains the requisite elements?
 - Including sharing nonpublic personal information with both affiliates and non-affiliates; sharing of information about those who are no longer customers; and protecting nonpublic personal information?
- Management adequately vets its privacy policies so that consumer information is properly categorized and non-public personal information sharing practices are properly treated as subject to opt out or exceptions to opt outs?
- Development efforts are coordinated so that information policies and practices match up with controls and system capabilities, including those systems provided by outside contractors?

Notices – Initial and Annual: As part of the plan, will management assure that

- Initial and annual notices are drafted to reflect the new policies with due regard for clarity and understandability?
- The rule's requirements concerning delivery, retention/accessibility and the appropriateness of utilizing the Simplified and/or Short form notices have been considered?

Opt-out Procedures (if applicable): As part of the plan, does management

- Determine the means by which it will enable an individual to opt out of information sharing, the “reasonableness” of such method(s) and the appropriateness of corresponding time periods for exercising opt out rights?
- Decide whether to afford customers partial opt-out rights and assure that systems are capable of handling that level of complexity?
- Construct systems adequate to track consumer information sharing choices?
- Prepare opt-out notices to meet the standards of being clear and conspicuous?

Third Party Concerns: As part of the plan, is management attentive to the need

- To draft new contract language for certain third party agreements that cover information sharing in order to adequately cover restrictions on reuse as required?
- To contract with responsible third parties who will abide by reuse and re-disclosure restrictions for information shared with them?
- To have controls for assuring the institution abides by reuse and re-disclosure restrictions for non-public personal information received by it from other financial institutions?
- For service providers to assimilate and meet the institution’s privacy policies in conducting any out-sourced compliance obligations?

Privacy Training Program: As part of the plan, does management

- Establish programs to train personnel in the handling of consumer information under the institution’s new privacy policies?
- Prepare materials for customer representatives to properly respond to consumer inquiries about the institution’s privacy plans, policies and practices?

IMPLEMENT compliant privacy policies

The plan should afford adequate time to test, implement and monitor the institution’s privacy policies and practices, to issue the requisite notices, and to allow a reasonable time for customers to exercise any available opt-out rights. Therefore, as part of the plan

- Is there a schedule for issuing initial and opt-out notices that leaves a reasonable time for customers to exercise their rights prior to the compliance deadline?
- Are the requirements of the privacy rule and the standards of related security and FCRA rules being coordinated during implementation to achieve comprehensive compliance?
- Will management prepare systems to process the influx of initial opt-outs?
- Will management have monitoring procedures in place to assure adherence to new policies?
- Will management have systems ready to demonstrate compliance to regulators and meet institution record retention policies?

- Will management take steps to assure that consumer relations representatives, and other personnel dealing with the retail customer, are fully prepared to respond to customer privacy inquiries?
- Are means of testing compliance before the deadline adequate for the sophistication of the institution's proposed policies and systems?
- Are service bureau systems that are relied on for fulfilling the institution's compliance obligations tested to assure compatibility with institution privacy policies and regulatory standards?

DIRECTIONS TO EXAMINERS FOR CONCLUDING CHECK-UP

After considering the institution's plan in view of the complexity and sophistication of its operations and the time remaining to the compliance deadline, the examiner should make an assessment of the institution's preparedness for achieving timely compliance with the privacy rule. When the Check-up is conducted as part of an on-site examination, present the evaluation and any other pertinent observations at the compliance examination Board exit meeting.

Include a brief summary of your conclusions about institutional privacy preparedness in examination work papers. Identify any areas of noteworthy achievement or challenges. Where weakness is identified consider whether regulatory or other assistance would be helpful. Submit your summary to your regional office designated e-mail account with any suggestions for supervisory follow-up or agency assistance.

Provide feedback on the Privacy Preparedness Check-up process to the same e-mail account and include any suggestions to improve the process, particularly with respect to the 2001 review.

Further instructions on how to communicate an examiner's evaluation to an institution when the Check-up is conducted off-site will be provided in advance of the 2001 review.

September 18, 2000